

(19)



Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11) Publication number:

**0 391 261 A3**

(12)

**EUROPEAN PATENT APPLICATION**

(21) Application number: 90106071.5

(51) Int. Cl.<sup>5</sup>: **G07F 7/10**

(22) Date of filing: 29.03.90

(30) Priority: 03.04.89 JP 81571/89  
18.05.89 JP 122944/89  
18.05.89 JP 122945/89

(43) Date of publication of application:  
10.10.90 Bulletin 90/41

(84) Designated Contracting States:  
DE FR GB

(88) Date of deferred publication of the search report:  
09.10.91 Bulletin 91/41

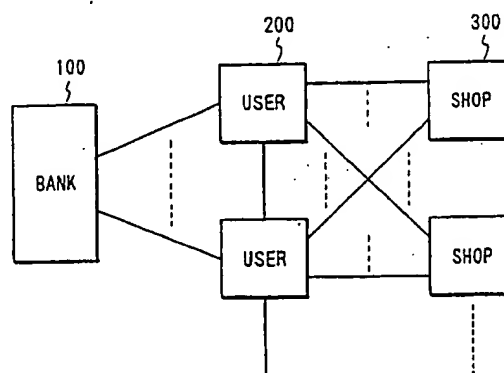
(71) Applicant: **NIPPON TELEGRAPH AND  
TELEPHONE CORPORATION**  
1-6 Uchisaiwaicho 1-chome Chiyoda-ku  
Tokyo(JP)

(72) Inventor: **Ohta, Kazuo**  
2-10-34 Yamanone  
Zushi-shi, Kanagawa(JP)  
Inventor: **Okamoto, Tatsuaki**  
94-2-5-503, Nagasawa  
Yokosuka-shi, Kanagawa(JP)

(74) Representative: **Blumbach Weser Bergen  
Kramer Zwirner Hoffmann Patentanwälte**  
Radeckestrasse 43  
W-8000 München 60(DE)

(54) Method and apparatus for implementing electronic cash.

(57) In an electronic cash implementing method, a user makes a bank apply a blind signature to user information  $V_i$  produced, by a one-way function, from secret information  $S_i$  containing identification information, thereby obtaining signed user information. Further, the user makes the bank apply a blind signature to information containing authentication information  $X_i$  produced, by a one-way function, from random information  $R_i$ , thereby obtaining signed authentication information. The user (200) uses an information group containing the signed user information, the signed authentication information, the user information and the authentication information, as electronic cash for payment to a shop. The shop (300) verifies the validity of the signed user information and the signed authentication information, and produces and sends to the user an inquiry. In response to the inquiry the user produces a response  $Y_i$  by using secret information and random information and sends it to the shop. Having verified the validity of the response the shop accepts the electronic cash.

*FIG. 1***EP 0 391 261 A3**



European  
Patent Office

## EUROPEAN SEARCH REPORT

Application Number

EP 90 10 6071

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
A	US-A-4 759 064 (CHAUM) * the whole document *	1-7,12-17	G 07 F 7/10
	---		
D,A	US-A-4 759 063 (CHAUM) * abstract; claims 1-20, 26-38; figures 1-7 *	1-20, 24-31, 37-48	
	---		
A	Advances in Cryptology - EUROCRYPT '88 May 1988, Berlin - DE Thomas Beth: "EFFICIENT ZERO-KNOWLEDGE IDENTIFICATION SCHEME FOR SMART CARDS" * pages 77 - 84 *	1-15	
	---		
A	Advances in Cryptology - CRYPTO '86 August 1986, Berlin - DE Amos FIAT et.al.: "How to Prove Yourself : Practical Solutions to & Signature Problems" * pages 186 - 194 *	1-20, 32-44	
	---		
P,A,D	EP-A-0 348 812 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) * the whole document *	1-52	
	-----		
The present search report has been drawn up for all claims			TECHNICAL FIELDS SEARCHED (Int. Cl.5)
			G 07 F H 04 L
Place of search		Date of completion of search	Examiner
The Hague		16 August 91	GUIVOL,O.
<b>CATEGORY OF CITED DOCUMENTS</b>			
X: particularly relevant if taken alone		E: earlier patent document, but published on, or after the filing date	
Y: particularly relevant if combined with another document of the same category		D: document cited in the application	
A: technological background		L: document cited for other reasons	
O: non-written disclosure		-----	
P: intermediate document		&: member of the same patent family, corresponding document	
T: theory or principle underlying the invention			